(12) UK Patent Application (19) GB (11) 2 369 753 (13) A

(43) Date of A Publication 05.06.2002

(21) Application No 0120169.8

(22) Date of Filing 17.08.2001

(30) Priority Data
(31) 0020323 (32) 17.08.2000 (33) GB

(71) Applicant(s)
Simoco International Limited
(Incorporated in the United Kingdom)
PO Box 24, St Andrews Road, CAMBRIDGE, CB4 1DP,
United Kingdom

(72) Inventor(s)
Mark Wentworth Rayne
Richard John Travett

(74) Agent and/or Address for Service
Frank B Dehn & Co
179 Queen Victoria Street, LONDON, EC4V 4EL,
United Kingdom

(51) INT CL[7]
H04Q 7/22 // H04Q 7/28

(52) UK CL (Edition T)
H4L LDPC

(56) Documents Cited
WO 01/95558 A1 WO 00/48416 A1
FI 000990256 A

(58) Field of Search
UK CL (Edition T) H4L LDPC
INT CL[7] H04L 9/00 29/06 , H04Q 7/22 7/28
Online Databases: WPI, EPODOC, JAPIO

(54) Abstract Title
Encrypted short data messages in mobile communications systems

(57) A Short Data Service (SDS) message 6 for sending an encrypted TETRA type-4 SDS message includes an encryption marker 7 that indicates that the message 6 includes an encrypted user message. The marker 7 is followed by an encryption header 8, which might consist of an encryption algorithm indicator, a key identifier, an initial value for synchronisation and a time stamp and check sum. The rest of the message follows the normal TETRA type-4 SDS message structure but is encrypted. The message may be sent as a type-4 SDS message using SDS-TL, or as an OTAR (over-the-air-rekeying) type short data message. Particular protocol identifiers (PID) 9 in the existing message structure may be used to indicate an encrypted message rather than an additional marker. The fully or partially encrypted SDS message may be packaged in a standard format short data message.

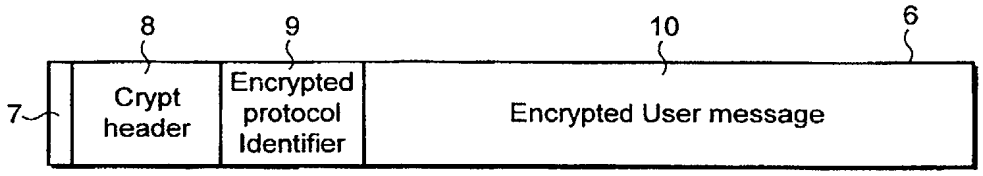

FIG. 4

GB 2 369 753 A

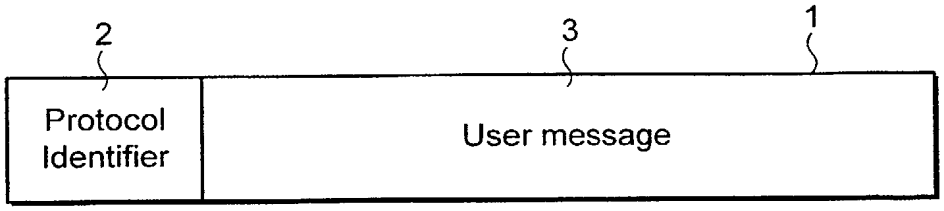

FIG. 1

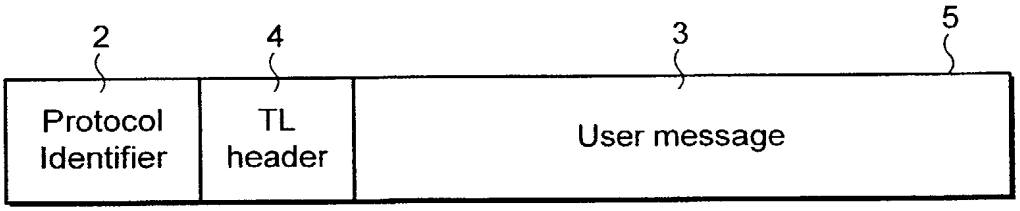

FIG. 2

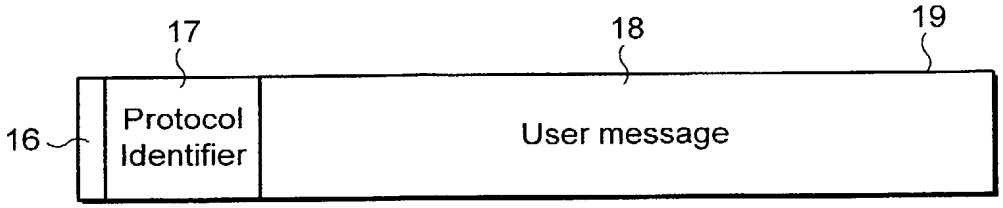

FIG. 3

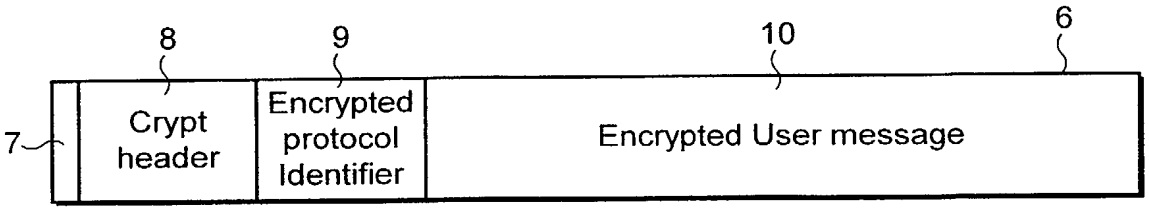

FIG. 4

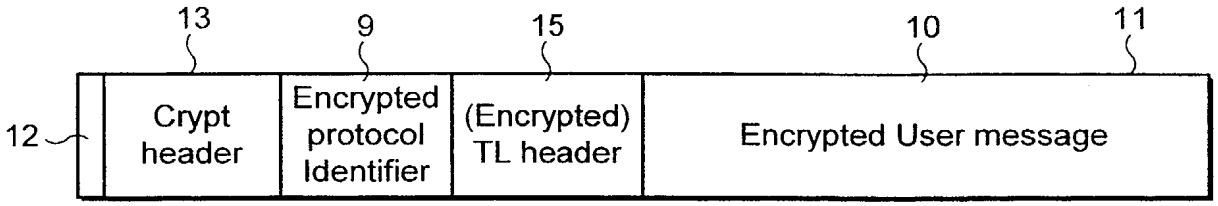

FIG. 5

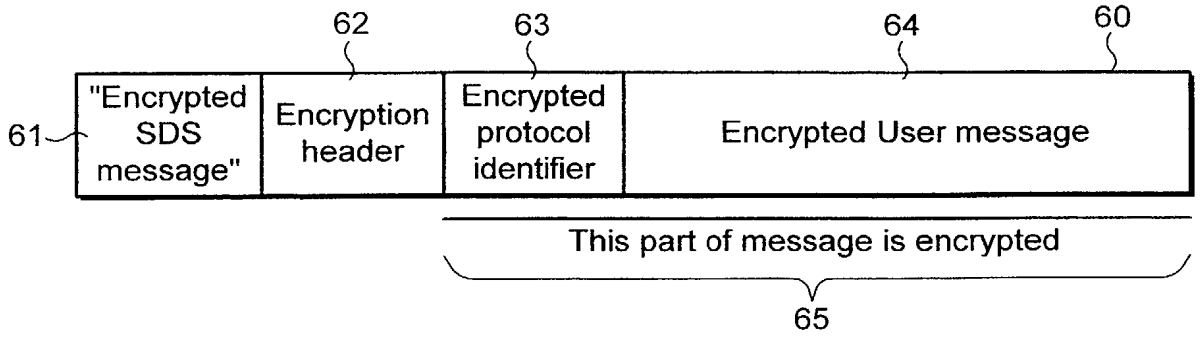

FIG. 6

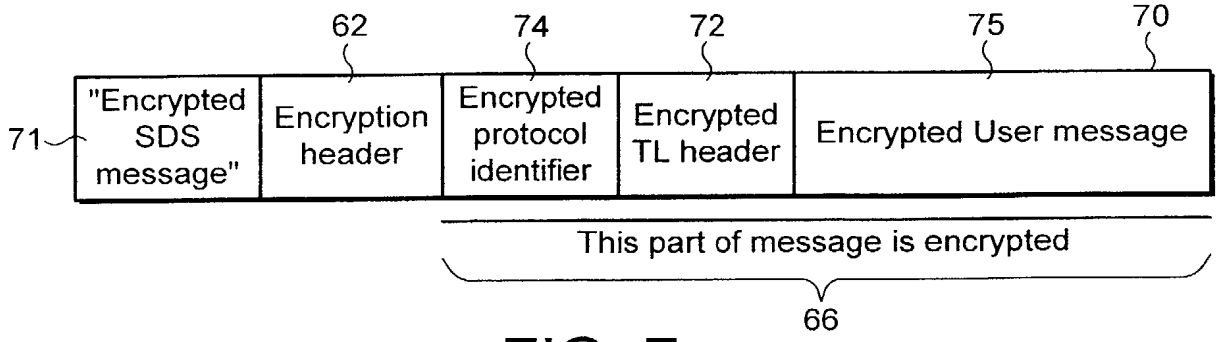

FIG. 7

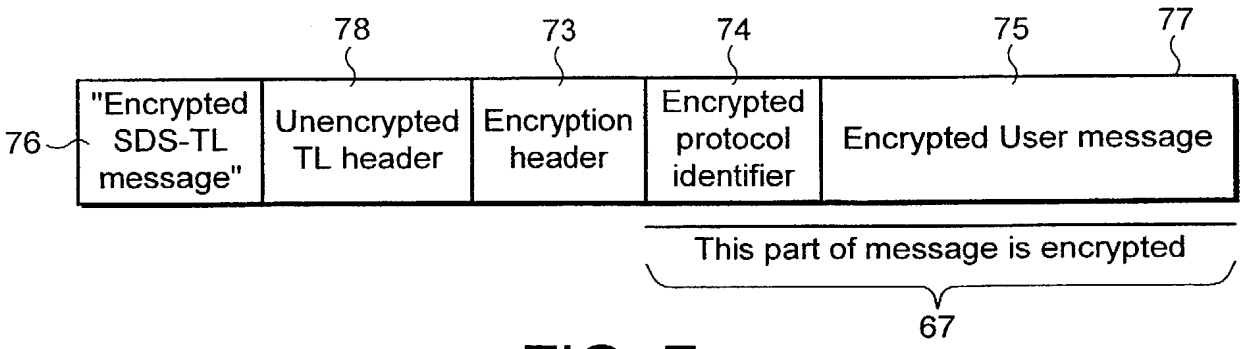

FIG. 7a

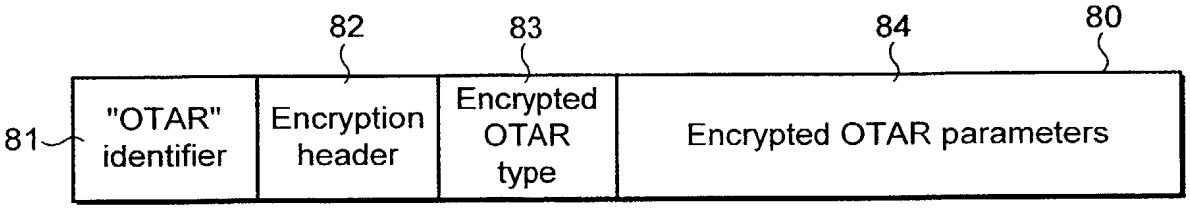

FIG. 8

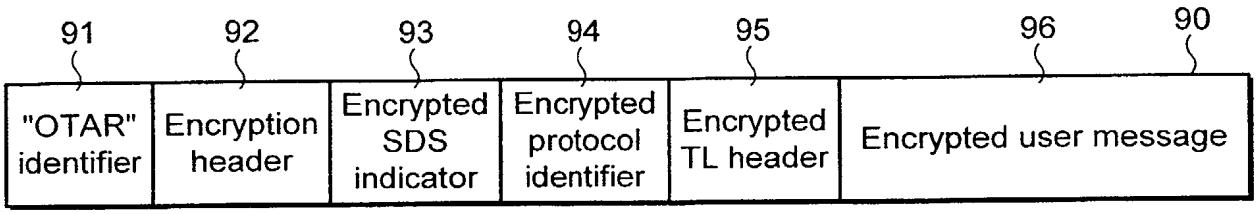

FIG. 9

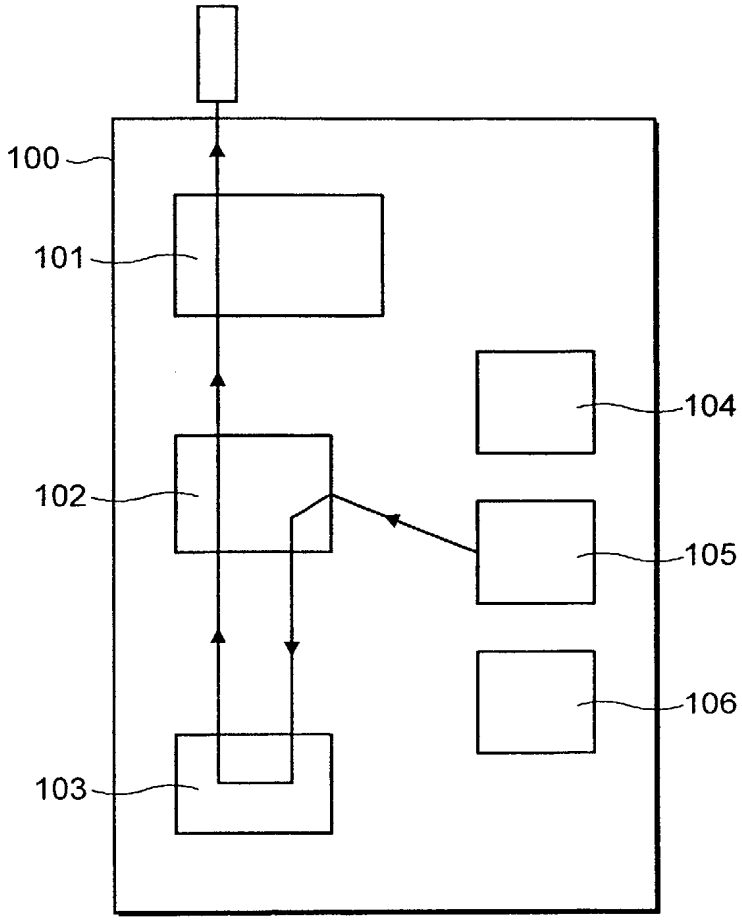

FIG. 10

Short Data Messages in Mobile Communications Systems

The present invention relates to the transmission of short data messages in mobile communications systems and in particular to the transmission of encrypted short data messages.

Many mobile communications systems support the transmission of short data messages in addition to voice communication, for, for example, carrying various types of data such as location information, text messages, status (e.g. of the radio-user) messages, telemetry, and alarm and warning messages. The Short Data Service (SDS) mechanism of the TETRA (TErrestrial Trunked RAdio) system (see, e.g., ETSI ETS 300 392-2) is one such short data message protocol. The Short Message Service (SMS) of the GSM (Global System for Mobile communications) system (see, e.g. Michel Mouly and Marie-Bernadette Pautet *The GSM System for Mobile Communications*, Cell & Sys, 1992 ISBN 2-9507190-0-7) is another. A similar short message service is available on MPT 1327 analogue trunked radio systems (see, e.g., MPT 1327 DTI).

It is becoming increasingly desirable to users of such communications systems to be able to encrypt their short data message transmissions. Some communications systems such as TETRA and GSM, automatically provide encryption over the air interface link (using in TETRA the standard air interface mechanism). However, it is becoming increasingly desirable to provide so-called 'end-to-end encryption' (i.e. to have the short data messages encrypted all the way from the sender to the recipient), as, for example, many users, such as public safety users, may not wish to rely on the security of the existing air interface encryption alone or may not trust the security of the fixed infrastructure.

However, many communications systems may not

directly support end-to-end encryption of short data messages. For example, while the TETRA system provides for air-interface encryption of all communications and end-to-end encryption of voice communication, the basic TETRA standard does not directly provide for end-to-end encryption of short data messages.

It is therefore an object of the present invention to provide mechanisms for helping radio systems offering short data message services, and in particular the TETRA system, to support end-to-end encryption of short data messages.

The Applicants have recognised in particular that where end-to-end encryption of short data messages is to be used, there must be some way of indicating to the recipient that the message includes an encrypted user or wanted message, so as to allow the recipient to process the message properly.

According to a first aspect of the present invention, there is provided a method of transmitting a short data message in a mobile communications system, comprising: when the short data message includes an encrypted message, including with the message an indication of that fact.

According to a second aspect of the present invention, there is provided an apparatus for transmitting a short data message in a mobile communications system, the apparatus comprising: means for, when the short data message includes an encrypted message, including with the message an indication of that fact.

In the present invention, when a short data message including an encrypted message is being transmitted, a separate indication of that fact (over and above the mere fact that the message itself is encrypted) is included with the short data message. This provides a convenient mechanism for indicating to the recipient the presence of an encrypted message in the short data

message.

The encryption indication could be placed anywhere in the message, although its position should be known to the receiver and is preferably therefore predetermined or its location previously indicated to the receiver (e.g. in an earlier message). The encryption indication is preferably placed towards the start of the message, e.g. it prefixes the encrypted short data message, and preferably precedes the user data in the message as this is more convenient where the messages may be of variable length (as it avoids the need to 'pad out' short messages in such circumstances).

The encryption indication is preferably not itself encrypted (to allow the recipient to read it).

The encryption indication could always be present and have two states, indicating respectively "encrypted message" and "unencrypted message". Alternatively, the indication could only be included with the message when it is encrypted or includes an encrypted message, but not otherwise (i.e. such that an unencrypted message is sent as normal).

If the message is not encrypted then the encryption indication, if present, would be set to "not encrypted", and the remainder of the message arranged as normal.

If the message is encrypted or contains an encrypted message, then the encryption indication would be included with it and set to "encrypted". The message to be encrypted would be encrypted and sent in an encrypted form in the message.

The message to be sent in an encrypted form can be any suitable such message that would normally be sent in a short data message but not necessarily always in an encrypted form (and for example may typically not be end-to-end encrypted in normal use, and/or, for example, would not be mandated to be sent in an encrypted form in the communications system in question). It would typically be a user message and/or an application

message, such as a text message, status message, position update, etc., that conveys or can convey information (e.g. wanted data) to another user of the system, and/or information from an end user or an end user application, rather than a message that conveys system data, such as an OTAR (over-the-air-rekeying) parameters message, that allows the system to operate but does not convey information proper to an end user.

The message to be sent in an encrypted form can be included in the short data message that is sent as desired. It could for example be formed by encrypting the original user message (e.g. text message, position update, GPS message, etc.), and then placing the encrypted user message in the "user message" field of the standard short data message format, with the remainder of the message being a 'normal' short data message (and including the usual short data message headers, etc.) in an unencrypted form, save for the presence of the encryption indication.

However, in a particularly preferred embodiment, the message to be sent in an encrypted form is first arranged in part or all of a normal short data message structure including some or all of the usual short data message system data headers, fields, etc, (and preferably at least one such header or field that conveys system operation data), and then the so-formed 'normal' short data message or short data message part is encrypted and included with the encryption indication in the actual short data message that is transmitted. Most preferably the encrypted normal short data message, or short data message part (preferably together with any remaining normal short data message headers, etc. that would be in a normal short data message, but which are not in the encrypted short data message part), is then packaged into a standard short data message structure, i.e. it is effectively placed in an apparently normal short data message wrapper, but which structure

(wrapper) includes the indication that the message it contains is an encrypted short data message. Upon seeing this indication, the recipient would then decrypt the original short data message and thereafter process it as a normal short data message.

Where the message is encrypted, it would typically also need to include further encryption information, for example in the form of an encryption header, to allow the recipient to decrypt the message. This encryption information or header preferably follows the encryption indication and is preferably in a predetermined or prearranged location in the message to allow its easy identification by the recipient. Where appropriate, it is preferably placed appropriately in the overall short data message "wrapper", outside the encrypted short data message. It is preferably placed towards the start of the message to allow for variable length messages, as discussed above.

The application of this invention to a TETRA system, could, for example, be as follows. TETRA provides a number of different short data message types: short "status" messages, free format SDS messages, and so-called type-4 SDS messages. The Applicants believe that it will most likely be desirable to use type-4 SDS messages for end-to-end encryption, as they can contain more user-defined data and therefore a longer user message, and as such have a greater capacity to carry the user data together with the necessary encryption synchronisation information such as the encryption synchronisation vector, etc., that may be needed to allow the message to be decrypted.

TETRA type-4 SDS messages are defined in ETSI ETS 300 392-2, clause 29. Figure 1 illustrates the format of one arrangement of a type-4 SDS message. The message 1 includes a leading "SDS Protocol Identifier" part or field 2 which comprises the first 8 bits of the message. The protocol identifier enables the SDS application in

the radio terminal to route the remaining contents of the SDS message to its intended application, and permits correct decoding of the message. (Possible applications include key management of end-to-end encryption (OTAR - over-the-air-rekeying), text messaging, wireless datagram protocol WAP, wireless control message protocol WCMP, managed TETRA Direct Mode, PIN authentication, and GPS position information (see, e.g. ETSI ETS 300-392-2, 29.4.3.8)). The user message 3 follows the protocol identifier 2.

Type-4 SDS messages can also use an additional protocol layer or facility known as the Short Data Service Transport Layer (SDS-TL) data transfer service (see, e.g., ETSI ETS 300 392-2; 29, 29.4.1, 29.4.2, and Annex J). This additional protocol layer enhances the Short Data Service protocol and improves message transport reliability, etc, by providing protocol mechanisms for, for example, end-to-end acknowledgement, and store and forward functions. It also ensures that applications using this service interpret the user data in the same way.

When the SDS-TL protocol is in use, the short data message includes additional header information, in the form of an SDS-TL header. Figure 2 illustrates such a message 5. The SDS-TL header 4 is inserted after the protocol identifier 2, but before the user message 3. In a type-4 SDS message, the first bit of the protocol identifier 2 indicates if the SDS-TL protocol is in use (see, e.g., ETSI ETS 300 392-2; 29.4.1 and Annex J) and therefore, for example, if a TL-header is included in the message.

Thus in the application of the present invention to a TETRA type-4 SDS message, the encryption indication could, for example, follow the protocol identifier and precede or follow the SDS-TL header, if any. The encrypted message would then follow and, have, when decrypted, the Standard Type-4 SDS format.

Where this invention is being used in a TETRA system, and the TETRA SDS-TL protocol is being used, the SDS-TL header may be encrypted if desired. However, the Applicants believe that it would generally be preferable not to encrypt the TL header, as it may be useful for the information it contains to still be readable by units of the system, e.g. the system infrastructure, or another mobile unit, which are not the intended recipient of the message (and so cannot decrypt the entire message). For example, the TL header may contain information which may be used by the system infrastructure to determine whether and how long to store or forward the message. It would be useful for the infrastructure still to be able to read this information even if it cannot, and is not intended to, decipher the entire message. However, if the TL header is encrypted, the infrastructure will be unable to decode it.

It may also be preferable for a mobile station to be able to read the TL header even if it is unable to decrypt the rest of the message. This is because the TL header may, for example, indicate whether the mobile station should report successful or failed reception of the message.

Indeed, in a preferred embodiment of the present invention, the intended recipient of the message (e.g. the recipient mobile station) reports back an error message, such as "encoding not supported", if it cannot decrypt the message. This could be done in a TETRA system using a short report (see, e.g., ETSI ETS 300-392-2, 29.4.3.10) used in the TETRA SDS-SHORT REPORT PDU (ETSI ETS 300-392-2; 29.4.2.3), or as a new value meaning "unable to decrypt message" in the "Delivery Status" parameter (ETSI ETS 300-392-2; 29.4.3.2) used in the SDS-REPORT PDU (ETSI ETS 300-392-2, 29.4.2.2).

In a TETRA, SDS-TL protocol, arrangement, whether or not the TL header is to be encrypted could, for

example, be predetermined, or pre-arranged in use (e.g. indicated to the recipient in an earlier message), or indicated by the encryption indication (e.g. by it taking a particular value) or within the encryption header (if any) included in the short data message.

Although the above described sequences of encryption indications, headers and user messages are preferred and convenient, in practice the order is unimportant so long as the relevant parties know the order to be used and to expect.

The encryption indication of the present invention could be given by adding it in the form of a marker or flag to the short data message, e.g. as an additional bit or bits at the beginning of the message (which could then otherwise have the normal short data message structure of the communications system, save for it being encrypted and possibly including the encryption header). This marker could, for example, be a single bit where only two encryption indication states (values) are needed, or more bits where more encryption indication states (values) are desired. In, for example, a system such as TETRA where it would be desirable to maintain the rest of the message in "octet-alignment", the marker could have a length of 8-bits, even though a field of eight bits may not be needed to support all the desired possible values of the encryption indication.

One drawback with simply adding an additional encryption indication marker to the existing short data message format is that the existing short data message format for the communications system may not support the addition of a marker in this way, e.g. it may not have the capacity for the extra bit or bits of the encryption marker. This is, for example, the case with TETRA type-4 SDS messages, as the capability of adding an extra marker in this way was not included when the type-4 SDS service was defined. Thus to add a marker

onto a standard type-4 SDS message in TETRA is no longer so easy to implement, as it would require some redefinition of the type-4 SDS service.

In particularly preferred embodiments of the present invention therefore, the encryption indication is given by including it within the existing short data message structure of the communications system, rather than by adding extra marker bits to the message structure. This avoids having to add an additional encryption marker to the short data message.

In one particularly preferred embodiment this is done by, for example, setting a value of an existing part or field of the short data message structure of the communications system to have a particular value or values. Many short data message arrangements include headers or similar parts or fields that contain "structure data", i.e. data required for the system to operate but not otherwise conveying user information proper, rather than proper user information or wanted data. These "structure data" elements would normally be set to particular values to convey particular information to allow the system to operate, but there are often spare, unused values to which these parts, headers, fields, etc., can be set to that have not been allocated particular meanings. These undefined values could instead be set to have the meanings "encrypted message" or "unencrypted message", etc, and then used to give the encryption indication.

In a TETRA system, using Type-4 SDS messages, this embodiment is in one arrangement preferably implemented by the encryption indication being particular protocol identifier values. Two encryption indicating protocol identifier values are preferred, one having the meaning "encrypted SDS message" and the other having the meaning "encrypted SDS-TL message", to enable the decrypting recipient station to detect the presence of the TL header when the SDS-TL protocol is being used.

In such an arrangement, when one of these protocol identifiers is used, it is preferably followed by the encryption header (if any) and then an encrypted version of the original message before the encryption was added, i.e. an encrypted message containing the true protocol identifier, SDS-TL header (if any) and the user message. In other words, the original message is effectively formatted as usual and then encrypted, and then the encrypted message mapped onto the usual SDS message format, but with the so-formed message having a special protocol identifier value that identifies it as containing an encrypted SDS message.

As discussed above, while it may generally be preferable to keep the TL-header unencrypted, in some circumstances, it may be desirable to encrypt it. It is preferably therefore possible for the recipient to determine if the TL-header is encrypted.

This could be achieved, for example, by having three different protocol identifier values, representing "encrypted SDS message", "encrypted SDS-TL message with unencrypted TL header", and "encrypted SDS-TL message with encrypted TL header". An infrastructure seeing, for example, the protocol identifier "encrypted SDS-TL message with unencrypted TL header" would then be able to look for the TL-header and manage the message in the same way as any other SDS-TL message.

However, the Applicants have recognised that in a TETRA system, a protocol identifier having its most significant bit set to "0" indicates to the system infrastructure and mobile stations that they should not attempt to read a TL header, whereas as a "1" in the most significant bit indicates that a TL header should be looked for (see, e.g., ETSI ET3 300-392-2; Annex J). Thus as a TL header should not be read in an encrypted SDS message and an encrypted SDS-TL message with an encrypted TL header, a protocol identifier with its most significant bit set to "0" can be used to indicate and

to allow the system to process correctly such messages. As the TL header should be looked for in an encrypted SDS-TL message with an unencrypted TL header, a protocol identifier with its most significant bit set to "1" can be used to indicate and to allow the system to process correctly such messages. In this way only two protocol identifier values are needed to indicate adequately the above three possible message states.

Thus, in a particularly preferred embodiment, two, and preferably only two, protocol identifier values are used to indicate encryption, one having its first (most significant) bit set to "0" (zero) which is used for encrypted SDS messages and encrypted SDS-TL message with an encrypted TL-header, and the other having its first (most significant) bit set to "1" (one) which is used for encrypted SDS-TL messages with an unencrypted TL-header.

Thus any SDS-TL message in which the TL header is unencrypted is preferably sent with a protocol identifier having its most significant bit set to "1", so that the recipients know to look for the TL header. An SDS-TL message in which the TL-header is encrypted is preferably sent with a protocol identifier value having a "0" as its most significant bit (as would be an encrypted SDS message), thereby effectively instructing a recipient not to look for a TL header. In this latter case, the fact that the message is in fact an SDS-TL message with an encrypted TL-header will become apparent when the message is decrypted, because the protocol identifier of the original message will then be visible. The message may then be decoded, managed, acknowledged, and disposed of as with any normal unencrypted type-4 SDS message.

Although it is preferred to use two or three and preferably only two protocol identifier values in this arrangement as discussed above, more such values could be used if it is for example desired to use different

protocol identifier values for different types of encrypted messages. Thus protocol identifier values (other than those already defined for another purpose) may be predefined to indicate, for example, the type of encrypted message that follows, such as whether it is an encrypted text message, an encrypted GPS message, etc. These protocol identifier values preferably have their most significant bits set to "0" or "1", to indicate the presence of an unencrypted TL-header as appropriate, as discussed above.

Thus more generally speaking, the encryption indication of the present invention can also be used to indicate the type of the encrypted message, if desired, e.g. by giving it different values depending on the type of encrypted message.

In another preferred embodiment of the present invention the encryption indication and the encrypted SDS message is effectively sent via an OTAR (over-the-air-rekeying) type short data message.

When applying this arrangement to TETRA type-4 SDS messages, rather than using special protocol identifier values as the encryption indication, the encryption indication is preferably included as a particular "OTAR" (over-the-air-rekeying) type parameter in an OTAR SDS message structure. In other words, the encrypted message is placed into the normal OTAR SDS message structure, but the OTAR command type parameter that is included in the OTAR SDS message structure is set to a value that has a new defined meaning to indicate that the remainder of the message is an encrypted type-4 SDS message, and not an OTAR instruction at all, in response to which the recipient will then process the decrypted message as a normal unencrypted type-4 SDS message.

In this arrangement, the SDS message would be given the standard "OTAR" protocol identifier, and the normal OTAR encryption header would typically then follow. The special encrypted OTAR type parameter indicating an

encrypted SDS message then preferably follows and is followed by the original SDS message (including its protocol identifier, etc.) in an encrypted form.

In this arrangement, as the encryption indication (i.e. the special OTAR command type) and the original message is encrypted inside the OTAR message, it would not be possible for a recipient or other part of the system to determine whether a TL header is present or if it is encrypted, until the rest of the message has been decrypted. Thus in this arrangement, the TL header has to be encrypted (unless the OTAR message has its own unencrypted SDS-TL header).

In another preferred embodiment, the encryption indication is placed inside the user message, (preferably at its start), or the user message part, of the short data message structure, rather than being added as a marker to the overall message. The encryption header, if any, would then preferably also be included in the user message part, at a convenient, e.g. predetermined place, e.g. immediately after the encryption indication or at the end of the message. The encrypted actual user message or data would then be placed in the user message part appropriately (e.g. follow the encryption indication and header).

When implementing this embodiment in a TETRA type-4 SDS arrangement, the encryption indicator in the user message preferably immediately follows the protocol identifier of a Type-4 SDS message, or the TL header of a type-4 SDS-TL message, as appropriate. The encryption indicator could, for example, be a particular Text Coding Scheme Value, e.g. any such value in which the most significant bit is set to "1" (one) (as the most significant bit is currently reserved in TETRA) (see, for example, ETSI ETS 300-392-2; 29.5.2.3 and 29.5.3.3).

Short data messages in accordance with the present invention can be assembled and transmitted as desired. In a particularly preferred embodiment, as discussed

above, such transmission comprises the basic user message (e.g. GPS message) being formed, and then packaged in the relevant short data message (e.g. TETRA SDS or SDS-TL) format. The so-formatted message is then encrypted.

The need for encryption can be indicated, for example, by the user. Alternatively or additionally, it could be predetermined that certain messages should be encrypted or should be encrypted when certain predetermined conditions are met. For example, it is usually desirable that position information messages in particular are encrypted. Additionally or alternatively, the destination of the message could be used to trigger end-to-end encryption, and/or to at least select the appropriate encryption key. (However, it is preferred that the application determines the use of encryption.) Preferably, if an encryption key is not available for a particular destination, the message is inhibited.

The so-encrypted message is then further packaged into the relevant short data message format, but with the encryption indication included in it (e.g. by setting a parameter within the encrypted message or the formed short data message to have a particular value), together with, if appropriate, a cryptographic header indicating the parameters to be employed for decryption. The so-assembled short data message can then be passed for transmission over the radio interface.

Receiving and decrypting an incoming short data message containing an encrypted message would follow the reverse process.

Thus according to a third aspect of the present invention, there is provided a method of transmitting an encrypted short data message in a mobile communications system that supports short data message transmission, the method comprising:

forming a message to be transmitted;

packaging the formed message in a standard short data message format for the communications system;

encrypting all or part of the so-formed short data message;

packaging the so-encrypted short data message, or the so-encrypted short data message part and the remaining unencrypted part of the so-formed short data message, in a standard short data message format of the communications system;

including with the so-packaged short data message an indication that the message contains an encrypted short data message or short data message part; and

transmitting the so-constructed short data message.

According to a fourth aspect of the present invention, there is provided an apparatus for transmitting an encrypted short data message in a mobile communications system that supports short data message transmission, the apparatus comprising:

means for forming a message to be transmitted;

means for packaging the formed short data message in a standard short data message format for the communications system;

means for encrypting all or part of the so-formed short data message;

means for packaging the so-encrypted short data message, or the so-encrypted short data message part and the remaining unencrypted part of the so-formed short data message, in a standard short data message format of the communications system;

means for including with the so-packaged short data message an indication that the message contains an encrypted short data message or short data message part; and

means for transmitting the so-constructed short data message.

These aspects of the present invention can include any one or more of the preferred features discussed

above. For example, in the case of a TETRA system, the standard short data message format that the original message is packaged into would be either the SDS or SDS-TL format (in which case the TL-header could be encrypted or unencrypted as desired), and the encryption indication could be, for example, a particular protocol identifier value which is prepended to the (encrypted or part-encrypted) original short data message when it is re-packaged into the appropriate short data message format.

In a preferred embodiment the original short data message is marked with a temporary identity tag before it is encrypted, which tag is unaltered by the encryption process, so that the apparatus can identify the encrypted short data message and, for example, send it to the correct destination.

The present invention also extends to the transmission and/or reception in a TETRA system of type-4 SDS messages having any or all of the structures described herein, and to suitable apparatus for such transmission and/or reception.

The methods in accordance with the present invention may be implemented at least partially using software e.g. computer programs. It will thus be seen that when viewed from further aspects the present invention provides computer software specifically adapted to carry out the methods hereinabove described when installed on data processing means, and a computer program element comprising computer software code portions for performing the methods hereinabove described when the program element is run on data processing means. The invention also extends to a computer software carrier comprising such software which when used to operate a radio system or unit comprising a digital computer causes in conjunction with said computer said system or unit to carry out the steps of the method of the present invention. Such a computer

software carrier could be a physical storage medium such as a ROM chip, CD ROM or disk, or could be a signal such as an electronic signal over wires, an optical signal or a radio signal such as to a satellite or the like.

It will further be appreciated that not all steps of the method of the invention need be carried out by computer software and thus from a further broad aspect the present invention provides computer software and such software installed on a computer software carrier for carrying out at least one of the steps of the methods set out hereinabove.

A number of preferred embodiments of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 shows the structure of a TETRA type-4 SDS message;

Figure 2 shows the structure of a TETRA type-4 SDS-TL message;

Figure 3 shows a TETRA type-4 SDS message with a leading encryption marker in accordance with a first embodiment of the present invention;

Figure 4 illustrates the sending of an encrypted type-4 SDS messages in accordance with the embodiment illustrated in Figure 3;

Figure 5 illustrates the sending of an encrypted type-4 SDS-TL message with a leading encryption marker in accordance with the first embodiment of the present invention;

Figure 6 illustrates the sending of an encrypted type-4 SDS message using a special protocol identifier in accordance with a second embodiment of the present invention;

Figure 7 illustrates the sending of an encrypted type-4 SDS-TL message using a special protocol identifier in accordance with the second embodiment of the present invention in which the TL header is

encrypted;

Figure 7a illustrates the sending of an encrypted type-4 SDS-TL message using a special protocol identifier in accordance with the second embodiment of the present invention in which the TL-header is not encrypted;

Figure 8 shows the format of a standard TETRA type-4 SDS OTAR message;

Figure 9 shows the inclusion of an encrypted type-4 SDS-TL message inside a type-4 SDS OTAR message in accordance with a third embodiment of the present invention; and

Figure 10 is a schematic diagram showing how an encrypted message is handled in a transmitter in accordance with an embodiment of the present invention.

Figures 3, 4 and 5 illustrate the inclusion of a leading encryption marker 16 (Figure 3), 7 (Figure 4) or 12 (Figure 5) in normal TETRA type-4 SDS messages to indicate the presence of an encrypted message or otherwise, in accordance with a first embodiment of the present invention. The encryption marker 16, 7, 12 could have a length of, for example, 1 bit, or, if it is desired to maintain the rest of the message in "octet-alignment" (as is specified in TETRA), a length of 8 bits.

In Figure 3, the message 19 is not encrypted, so the encryption marker 16 would indicate that fact and the remainder of the message then follows the usual type-4 SDS message structure, and therefore includes a leading protocol identifier 17 followed by the user message 18.

Figure 4 shows the structure of an SDS message 6 for sending an encrypted type-4 SDS message in accordance with the first embodiment of the invention. The message 6 includes an encryption marker 7 that indicates that the message 6 includes an encrypted user message (in this case that the protocol identifier and

user message are both encrypted). The marker is followed by an encryption header 8, which might typically consist of an encryption algorithm indicator, a key identifier, an initial value (IV) for synchronisation, and, optionally, a time stamp and a check sum. This encryption header could have a length of, for example, 8 to 16 octets. The rest of the message follows the normal type-4 SDS message structure, but is encrypted. Thus it includes an encrypted protocol identifier 9 and the encrypted user message 10.

Figure 5 shows the structure of an SDS message 11 for sending an encrypted type-4 SDS-TL message when using a leading encryption indicator 12. Again, an encryption header 13 follows the encryption marker 12. In the arrangement in Figure 5, the rest of the message is then encrypted and includes the encrypted protocol identifier 9, an encrypted TL-header 15, and an encrypted user message 10. However, as discussed above, the TL-header may be left unencrypted, in which case the TL-header would follow the encryption header 13 and come before the encrypted protocol identifier 9. The use of an unencrypted TL-header may be, for example, pre-arranged, or where the TL-header can be selectively unencrypted, this fact may be indicated appropriately in the encryption marker, e.g. by defining a third value for it.

Figures 6, 7 and 7a show a second embodiment of the present invention which does not require any addition of an encryption marker to the format of normal TETRA SDS messages. This is accomplished by using two special "protocol identifier" values with the meanings "encrypted SDS message" and "encrypted SDS-TL message". The encryption header then immediately follows the encrypted SDS message protocol identifier and thereafter, the format is the same as for unencrypted messages. (Alternatively, the encrypted SDS-TL message protocol identifier could be followed by the unencrypted

TL-header, so that the infrastructure in particular can, for example, treat the message like any other SDS-TL message.)

Figure 6 shows the structure of an SDS message 60 for sending an encrypted type-4 SDS message in accordance with this embodiment. The message includes a leading special protocol identifier 61 indicating "encrypted SDS message", followed by the encryption header 62. There then follows the remaining encrypted part 65 of the message, which includes the normal, 'true' SDS protocol identifier 63 (which is now encrypted) and the encrypted user message 64. (Thus it can be seen that the parts 63 and 64 are effectively an encrypted normal SDS message which is then repackaged together with the encryption header 62, into an SDS 'wrapper' having the special "encrypted SDS message" protocol identifier 61.)

Figure 7 shows the structure of an SDS message 70 for sending an encrypted type-4 SDS-TL message in this embodiment with the TL-header encrypted. In that case, the special protocol identifier 71 "encrypted SDS message" heads the message 70 and is followed by an encryption header 62. The remaining part 66 of the message is encrypted and follows the same format as a normal SDS message, and thus includes the true protocol identifier 74 (which is encrypted), the TL-header 72 (which is encrypted) and the encrypted user message 75.

Figure 7a shows the structure of an SDS message 77 for sending an encrypted type-4 SDS-TL message, which is arranged in accordance with this embodiment but in which the TL-header is not encrypted. The message 77 includes the special protocol identifier 76 indicating "encrypted SDS-TL message", which is followed by the unencrypted TL-header 78 (which is preferably placed next, so that, for example, the infrastructure in particular can treat the message like any other SDS-TL message (although in practice the actual sequence of headers and indicators

is unimportant so long as all parties know the sequence in advance)), and then the encryption header 73. The remaining part 67 of the message is then encrypted and includes the original, true protocol identifier 74 and the user message 75.

Figures 8 and 9 illustrate a third preferred embodiment of the present invention, which also uses a standard overall SDS message format for transmitting the encrypted SDS message. In this embodiment, the encrypted type-4 SDS message is effectively sent as (wrapped in) a type-4 SDS OTAR message.

Figure 8 illustrates the format of a standard TETRA type-4 SDS OTAR message. The message 80 includes an OTAR identifier 81 followed by the OTAR encryption header 82, an encrypted OTAR type code 83 and then a part 84 containing the encrypted OTAR parameters.

Figure 9 shows a modification of such a message to allow the transmission of an encrypted type-4 SDS-TL user message. In this case, the message 90 still includes the OTAR protocol identifier 91, which is still followed by the standard OTAR encryption header 92. However, after the encryption header 92, a special encrypted OTAR-type parameter 93 which acts as an "encrypted SDS message" indicator is sent. This OTAR command type is a new instruction, indicating that the remainder of the message is a type-4 SDS message and not an OTAR instruction at all. The remainder of the message 90 then comprises the encrypted "normal" SDS-TL user message, which effectively replaces the encrypted OTAR parameters in the OTAR-type message, and includes the true protocol identifier 94 followed by the TL-header 95 and the user message 96.

Upon receipt of this type of message, the type-4 SDS application in the radio unit would initially pass the message to the end-to-end cryptographic module, as it appears to be a normal OTAR message. Upon reading of the new OTAR command type 93 indicating an encrypted SDS

message, the cryptographic module would return the decrypted message to the type-4 SDS application for subsequent processing.

Figure 10 shows schematically how encrypted short data messages in accordance with the present invention may be routed through a TETRA radio unit 100. The unit includes a GPS (Global Positioning System) unit 105, other modules 104, 106 which could be other applications such as text messaging or managed Direct Mode which may wish to send a received encrypted short data messages from time-to-time, a short data service (SDS) application unit 102, a cryptographic unit 103, and the normal TETRA lower protocol layers 101 which prepare the message for transmission over the radio interface.

Figure 10 illustrates the situation where it is desired to send a GPS short data message that is encrypted. The basic GPS message is sent from the GPS unit 105 to the SDS application unit 102. The SDS application unit packages the message in standard SDS or SDS-TL format (as required). The SDS application unit 102 also determines whether the message should be encrypted, possibly by noting an instruction from the GPS unit 105 or, for example, by reading some pre-stored information requiring messages from the GPS unit to be encrypted.

If the message is to be encrypted, the SDS application unit 102 sends the SDS message to the cryptographic unit 103. The cryptographic unit 103 encrypts the entire SDS or SDS-TL message and prepends the cryptographic header indicating the parameters to be employed for decryption. The cryptographic unit 103 then returns the message to the SDS application unit 102. The SDS application unit 102 then prepends the protocol identifier value "encrypted SDS message" or "encrypted SDS-TL message", etc., as appropriate, and passes the entire message to the lower protocol layers 101 for transmission over the radio interface. (In an

alternative arrangement, the cryptographic unit 103 could prepend the "encrypted message" indication and then pass the message to the SDS application unit 102. This may be preferable, as it reduces the risk of unencrypted material being inadvertently mixed into encrypted material by the SDS application unit.)

If desired, the SDS application unit 102 can mark the SDS message with a temporary identity tag before passing it to the cryptographic unit 103. The cryptographic unit should then leave this tag unaltered, so that the SDS application unit 102 can identify the encrypted SDS and send it to the correct destination (for example as requested by the originating GPS application unit 105).

Receiving and decrypting an incoming SDS message would follow the reverse process, except that when the unencrypted SDS message is passed from the encryption unit 103 to the SDS application unit 102, the SDS application unit 102 would be able to read the true protocol identifier within the message and thereby pass the SDS message to its target application (e.g. a text displaying application unit, or, in the case of position information, a display unit displaying the locations of mobile units on a map on a screen).

As can be seen from the above, the present invention provides a number of ways of end-to-end encrypting TETRA SDS messages. At least some of the preferred embodiments build on the existing TETRA SDS mechanism by adding end-to-end encryption to the existing SDS type-4 message structure.

Although the invention has been described with particular reference to the TETRA system, as will be appreciated by those skilled in the art, it could be applied to any service carrying short data messages, such as GSM, MPT 1327, UMTS (Universal Mobile Telephone Service), TETRAPOL, etc, e.g. by placing an encrypted message inside a normal short data message format and by

setting a particular field, e.g. header, of the message to a new value to indicate an "encrypted message".

CLAIMS

1. A method of transmitting a short data message in a mobile communications system, comprising: when the short data message includes an encrypted message, including with the message an indication of that fact.

2. The method of claim 1, wherein the encryption indication precedes the encrypted message.

3. The method of claim 1 or 2, wherein the encryption indication is also used to indicate the type of the encrypted message.

4. The method of claim 1, 2 or 3, wherein the message to be sent in an encrypted form comprises a text message, status message, or a position update message.

5. The method of any one of claims 1 to 4, wherein the short data message which is transmitted is packaged in a standard short data message structure of the communications system.

6. The method of any one of claims 1 to 5, wherein the communications system is a TETRA system, and the short data message is sent as a type-4 SDS message.

7. The method of claim 6, wherein the message is sent as a type-4 SDS message using SDS-TL and the TL header is sent unencrypted.

8. The method of any one of claims 1 to 7, wherein the transmitted short data message includes encryption information to assist the recipient to decrypt the message.

9. The method of claim 8, wherein the encryption

information follows the encryption indication and is located outside the encrypted part of the short data message.

10. The method of any one of the preceding claims, further comprising the recipient of the message reporting back an error message if it cannot decrypt the message.

11. The method of claim 10, wherein the communications system is a TETRA system, and the error message is sent as a short report in the TETRA SDS-SHORT REPORT PDU, or as a particular value of the Delivery Status parameter used in the SDS-REPORT PDU.

12. The method of any one of the preceding claims, wherein the encryption indication and the encrypted message are sent via an OTAR (over-the-air-rekeying) type short data message.

13. The method of claim 12, wherein the communications system is a TETRA system, comprising: sending the message as a TETRA type-4 SDS OTAR message, and providing the encryption indication as a particular OTAR-type parameter in the OTAR SDS message structure.

14. The method of any one of the preceding claims, wherein the encryption indication is placed inside the user message part of the short data message structure.

15. The method of any one of the preceding claims, wherein the encryption indication is given by adding it in the form of a marker or flag to the short data message.

16. The method of any one of claims 1 to 14, wherein the encryption indication is given by setting a value of

an existing part or field of a short data message structure of the communications system to a particular value or values.

17. The method of any one of claims 1 to 14 or of claim 16, wherein the communications system is a TETRA system, comprising using particular protocol identifier (PID) values as the encryption indication.

18. The method of claim 17, wherein two encryption indicating protocol identifier values are used, one to indicate an encrypted SDS message, and the other to indicate an encrypted SDS message using SDS-TL.

19. The method of claim 17, wherein two protocol identifier values are used to indicate an encrypted message, one having its first bit set to "0" which is used for encrypted SDS messages and encrypted SDS messages using SDS-TL with an encrypted TL-header, and the other protocol identifier value having its first bit set to "1" and which is used for encrypted SDS messages using SDS-TL with an unencrypted TL-header.

20. The method of any one of claims 17 to 19, wherein the short data message comprises the encryption indicating protocol identifier, followed by an encrypted part of the short data message containing the true protocol identifier for the message that is encrypted and the encrypted message.

21. The method of any one of the preceding claims, comprising arranging the message to be sent in an encrypted form in part or all of a normal short data message structure for the communications system including some or all of the usual short data message system data headers and fields; encrypting the so-formed short data message or short data message part; and

including the encrypted so-formed short data message or short data message part with the encryption indication in the short data message that is transmitted.

22. A method of transmitting an encrypted short data message in a mobile communications system that supports short data message transmission, the method comprising:

forming a message to be transmitted;

packaging the formed message in a standard short data message format for the communications system;

encrypting all or part of the so-formed short data message;

packaging the so-encrypted short data message, or the so-encrypted short data message part and the remaining unencrypted part of the so-formed short data message, in a standard short data message format of the communications system;

including with the so-packaged short data message an indication that the message contains an encrypted short data message or short data message part; and

transmitting the so-constructed short data message.

23. The method of claim 22, wherein the communications system is a TETRA system, and the standard short data message format that the original message is packaged into is either the SDS message format or the SDS message using SDS-TL format, and the encryption indication is a particular protocol identifier value which is prepended to the encrypted or part-encrypted original short data message when it is re-packaged into the appropriate short data message format.

24. The method of claim 21, 22 or 23, further comprising marking the original short data message with a temporary identity tag before it is encrypted, which tag is unaltered by the encryption process, so that the apparatus can identify the encrypted short data message.

25. The method of claim 21, 22, 23 or 24, further comprising the features of any one of claims 1 to 20.

26. The method of any one of the preceding claims, wherein the communications system is a TETRA system, comprising:

forming the message to be encrypted;

providing a protocol identifier value for the message to be encrypted;

encrypting the message to be encrypted and its protocol identifier value;

placing the encrypted message and encrypted protocol identifier value in a TETRA SDS message format; and

providing the so-formed SDS message with a further protocol identifier value that identifies the SDS message as containing an encrypted message.

27. A method of operating a TETRA mobile communications system, comprising transmitting or receiving a type-4 SDS message in accordance with any one of claims 1 to 26.

28. An apparatus for transmitting a short data message in a mobile communications system, the apparatus comprising: means for, when the short data message includes an encrypted message, including with the message an indication of that fact.

29. The apparatus of claim 28, wherein the encryption indication precedes the encrypted message.

30. The apparatus of claim 28 or 29, wherein the short data message which is transmitted is packaged in a standard short data message structure of the communications system.

31. The apparatus of any one of claims 28 to 30, wherein the communications system is a TETRA system, and the short data message is sent as a type-4 SDS message.

32. The apparatus of claim 31, wherein the message is sent as a type-4 SDS message using SDS-TL and the TL header is sent unencrypted.

33. The apparatus of any one of claims 28 to 32, further comprising means for including in the transmitted short data message encryption information to assist the recipient to decrypt the message.

34. The apparatus of any one of claims 28 to 33, wherein the encryption indication and the encrypted message are sent via an OTAR (over-the-air-rekeying) type short data message.

35. The apparatus of claim 34, wherein the communications system is a TETRA system, further comprising: means for sending the message as a TETRA type-4 SDS OTAR message, and means for providing the encryption indication as a particular OTAR-type parameter in the OTAR SDS message structure.

36. The apparatus of any one of claims 28 to 35, further comprising means for placing the encryption indication inside the user message part of the short data message structure.

37. The apparatus of any one of claims 28 to 36, further comprising means for adding the encryption indication in the form of a marker or flag to the short data message.

38. The apparatus of any one of claims 28 to 36, comprising means for giving the encryption indication by

setting a value of an existing part or field of a short data message structure of the communications system to a particular value or values.

39. The apparatus of any one of claims 28 to 36 or of claim 38, wherein the communications system is a TETRA system, comprising means for using particular protocol identifier (PID) values as the encryption indication.

40. The apparatus of claim 39, wherein two encryption indicating protocol identifier values are used, one to indicate an encrypted SDS message, and the other to indicate an encrypted SDS message using SDS-TL.

41. The apparatus of claim 39 or 40, wherein the short data message comprises the encryption indicating protocol identifier, followed by an encrypted part of the short data message containing the true protocol identifier for the message that is encrypted and the encrypted message.

42. The apparatus of any one of claims 28 to 41, comprising means for arranging the message to be sent in an encrypted form in part or all of a normal short data message structure for the communications system including some or all of the usual short data message system data headers and fields; means for encrypting the so-formed short data message or short data message part; and means for including the encrypted so-formed short data message or short data message part with the encryption indication in the short data message that is transmitted.

43. An apparatus for transmitting an encrypted short data message in a mobile communications system that supports short data message transmission, the apparatus comprising:

means for forming a message to be transmitted;

means for packaging the formed short data message in a standard short data message format for the communications system;

means for encrypting all or part of the so-formed short data message;

means for packaging the so-encrypted short data message, or the so-encrypted short data message part and the remaining unencrypted part of the so-formed short data message, in a standard short data message format of the communications system;

means for including with the so-packaged short data message an indication that the message contains an encrypted short data message or short data message part; and

means for transmitting the so-constructed short data message.

44. The apparatus of claim 43, wherein the communications system is a TETRA system, and the standard short data message format that the original message is packaged into is either the SDS message format or the SDS message using SDS-TL format, and the encryption indication is a particular protocol identifier value which is prepended to the encrypted or part-encrypted original short data message when it is re-packaged into the appropriate short data message format.

45. The apparatus of claim 42, 43 or 44, further comprising means for marking the original short data message with a temporary identity tag before it is encrypted, which tag is unaltered by the encryption process, so that the apparatus can identify the encrypted short data message.

46. The apparatus of claim 42, 43, 44 or 45, further

comprising the features of any one of claims 28 to 41.

47. The apparatus of any one of claims 28 to 46, wherein the communications system is a TETRA system, comprising:

means for forming the message to be encrypted;

means for providing a protocol identifier value for the message to be encrypted;

means for encrypting the message to be encrypted and its protocol identifier value;

means for placing the encrypted message and encrypted protocol identifier value in a TETRA SDS message format; and

means for providing the so-formed SDS message with a further protocol identifier value that identifies the SDS message as containing an encrypted message.

48. An apparatus for use in a TETRA mobile communications system, comprising means for transmitting or means for receiving a type-4 SDS messages in accordance with any one of claims 28 to 47.

49. A short data message for a mobile communications system, comprising: an encrypted message, and an indication that the short data message includes an encrypted message.

50. The short data message of claim 49, wherein the encryption indication precedes the encrypted message.

51. The short data message of claim 49 or 50, wherein the short data message is a TETRA type-4 SDS message.

52. The short data message of claim 51, wherein the message is a type-4 SDS message using SDS-TL and the TL header is unencrypted.

53. The short data message of any one of claims 49 to 52, further comprising encryption information to assist the recipient to decrypt the message.

54. The short data message of claim 53, wherein the encryption information follows the encryption indication and is located outside the encrypted part of the short data message.

55. The short data message of any one of claims 49 to 54, wherein the short data message is an OTAR (over-the-air-rekeying) type short data message.

56. The short data message of claim 55, wherein the short data message is a TETRA type-4 SDS OTAR message, and the encryption indication is a particular OTAR-type parameter in the OTAR SDS message structure.

57. The short data message of any one of claims 49 to 55, wherein the encryption indication is placed inside the user message part of the short data message structure.

58. The short data message of any one of claims 49 to 57, wherein the encryption indication is in the form of a marker or flag added to the short data message.

59. The short data message of any one of claims 49 to 57, wherein the encryption indication is comprised of particular value of a part or field of the short data message structure.

60. The short data message of any one of claims 49 to 57 or of claim 59, wherein the short data message is a TETRA short data message, and the encryption indication comprises a particular protocol identifier (PID) value.

61. The short data message of claim 60, wherein the short data message comprises the encryption indicating protocol identifier followed by an encrypted part of the short data message containing the true protocol identifier for the message that is encrypted and the encrypted message.

62. A computer program element comprising computer software code portions for performing the method of any one of claims 1 to 27 when the program element is run on data processing means.

63. A method of transmitting a short data message in a mobile communications system substantially as hereinbefore described with reference to any one of the accompanying drawings.

64. A method of operating a TETRA mobile communications system substantially as hereinbefore described with reference to any one of the accompanying drawings.

65. An apparatus for transmitting a short data message in a mobile communications system substantially as hereinbefore described with reference to any one of the accompanying drawings.

66. An apparatus for use in a TETRA mobile communications system substantially as hereinbefore described with reference to any one of the accompanying drawings.

67. A short data message substantially as hereinbefore described with reference to any one of Figures 3, 4, 5, 6, 7, 7a, and 9 of the accompanying drawings.

INVESTOR IN PEOPLE

Application No: GB 0120169.8 **Examiner:** Gareth Griffiths
Claims searched: All **Date of search:** 2 April 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): H4L (LDPC)

Int Cl (Ed.7): H04L 9/00, 29/06, H04Q 7/22, 7/28

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X, E	WO01/95558 A1	(MATSUSHITA) p.13 line 16 - p.14 line 15	1-4,8,15, 16,49-50, 53,58, 59,62
X, P	WO00/48416 A1	(SONERA) p.12 line 19 - p.13 line 23	1-4,8,9, 15,16,49, 50,53,54, 58,59,62
X	FI 990256 A	(SONERA)	1-4,8,9, 15,16,49, 50,53,54, 58,59,62

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.